CLAIMS

1. A system for detecting intrusions on a host, comprising:

   a) a sensor for collecting information including events and timestamps from a logfile; and

   b) an analysis engine configured to identify backward and forward time steps in the logfile, correlate the time steps with events, and assign a suspicion value to an event.

2. The system as recited in claim 1, wherein the analysis engine is configured to identify a time step as forward if a timestamp of an entry in the logfile is later than an preceding entry in the logfile, and identify a time step as backward if a timestamp of an entry in the logfile is earlier than an preceding entry in the logfile.

3. The system as recited in claim 1, wherein the analysis engine is further configured to use expected activity level in the directory to determine the suspicion value.

4. The system as recited in claim 1, further comprising a second sensor for collecting information including events and timestamps from a second logfile.

5. The system as recited in claim 4, wherein the analysis engine is configured to correlate a time step in the logfile with an event in the second logfile.

6. The system as recited in claim 1, wherein the analysis engine is further configured to filter out expected time steps from further analysis.

7. The system as recited in claim 6, wherein the analysis engine is configured to filter out expected backward time steps by correlating them to Network Time Protocol adjustments.

8. The system as recited in claim 6, wherein the analysis engine is further configured to compute an expected time drift resulting from a Network Time Protocol adjustment, and compare a forward time step in the logfile with the expected time drift.

9. The system as recited in claim 8, wherein the analysis engine is further configured to compute a standard deviation of the expected time drift.

10. The system as recited in claim 9, wherein the analysis engine is further configured to label time steps with weighted distributions.

11. The system as recited in claim 1, further comprising a user interface, and wherein the analysis engine is configured, upon correlating a time step to a record of an event in a logfile, to present the record to a user for labeling as to suspicion value.

12. The system as recited in claim 11, wherein the analysis engine is further configured to propagate the suspicion value to related events.

13. A system for detecting intrusions on a host, comprising:

a) a filesystem scanner configured to examine timestamps of files and directories in a filesystem; and

b) an analysis engine configured to compare timestamps of a directory and of files in the directory, and assign a suspicion value to the directory or file if the timestamps are inconsistent.

14. The system as recited in claim 13, wherein the analysis engine is configured to treat timestamps as inconsistent if the timestamp of the directory is later than the timestamp of any file in the directory.

15. The system as recited in claim 13, further comprising an archival source, wherein the filesystem scanner is configured to examine timestamps of files and directories from the archival source, and the analysis engine is further configured to compare the timestamps from the archival source to the timestamps of the directory and files in the directory.

16. A method for detecting intrusions on a host, comprising the steps of:

a) collecting information including events and timestamps from a logfile;

b) identifying backward and forward time steps in the logfile;

c) correlating the backward and forward time steps with events; and

d) assigning a suspicion value to an event.

17. A computer program product for detecting intrusions on a host, the computer program product being embodied in a computer readable medium having machine readable code embodied therein for performing the steps of:

a) collecting information including events and timestamps from a logfile;

b) identifying backward and forward time steps in the logfile;

c) correlating the backward and forward time steps with events; and

d) assigning a suspicion value to an event.